ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 681.518.25:004.056

В.М. ДУБОВОЙ, Г.Ю. ДЕРМАН

Вінницький національний технічний унівеерситет, Вінниця

ПІДХІД ДО ВИЗНАЧЕННЯ РІВНЯ БЕЗПЕКИ СИСТЕМИ, ЩО РОЗВИВАЄТЬСЯ

Анотація. Розрахунок ризику базується на прогнозі розвитку структури інформаційної сиситеми. Наведені деякі фактори і характеристики небезпеки неузгодженого розвитку. Для розрахунку ймовірності небезпеки використана експоненційно-мультиплікативна апроксимація. Для прогнозування розвитку використана модифікована логістична крива.

Ключові слова: інформаційна система (ІС), безпека інформаційної системи, розвиток.

Аннотация. Расчет риска базируется на прогнозе развития структуры информационной системы. Приведены некоторые факторы и характеристики опасности несогласованного развития. Для расчета вероятности опасности использована экспоненциально-мультипликативная аппроксимация. Для прогнозирования развития использована модифицированная логистическая кривая.
Текст аннотации.

Ключевые слова: информационная система (ИС), безопасность информационной системы, развитие.

Abstract. The calculation of risk based on forecasts of the structure of information system. The following are some factors and characteristics of risk inconsistent development. To calculate the probability of danger used exponentially-multiplicative approximation. To predict the development used a modified logistic curve.

Key words: information system, security of information system, development.

Вступ

Інформаційні системи, забезпечуючи постійно зростаючі потреби суспільства у отриманні, обробці, збереженні, пошуку та поданні інформації, знаходяться у стані відповідного постійного розвитку. При цьому розвиваються усі компоненти ІС: програмні і апаратні, призначені для передавання, зберігання і обробки інформації тощо. Розвиток має як параметричний характер (заміна окремих елементів ІС на інші з кращими параметрами), так і структурний (зміна функцій, кількості, якості елементів та зв'язків між ними). Будь-які зміни в ІС можуть приводити до погіршення рівня її безпеки. Таким чином, забезпечення такої стратегії розвитку ІС, при якому принаймні не погіршується рівень її безпеки, є важливою проблемою.

Наразі є низка міжнародних і національних стандартів та наукових досліджень з безпеки інформаційних систем (інформаційних технологій) [1, 2, 3, 4]. Відповідно до документа [4], який є основою організації системи безпеки інформаційних технологій у Росії і відповідає міжнародним стандартам безпеки [1, 2, 3], «Под безопасностью информационной технологии понимается состояние ИТ, определяющее защищенность информации и ресурсов ИТ от действия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз, а также способность ИТ выполнять предписанные функции без нанесения неприемлемого ущерба субъектам информационных отношений». Хоча це означення охоплює усі можливі випадки і наслідки порушення безпеки, проте на практиці розглядаються переважно випадки появи у складі ІС програмно-апаратного забезпечення, яке може містити джерело загрози або само по собі, або у разі зовнішніх злочинних дій. Проте важливим фактором зменшення рівня безпеки ІС може бути неузгоджений розвиток окремих компонентів ІС, при тому, що кожен компонент сам по собі не несе загрози безпеці.

Актуальність

На даний час існує багато моделей комплексного захисту інформаційних систем, а також великий вибір технічних та програмних засобів захисту інформації, методик інформаційної безпеки [5, 6], але відсутня методика визначення рівня безпеки саме систем, що розвиваються.

Рівень безпеки прийнято оцінювати величиною ризику R, а забезпечення безпеки – це процес управління ризиками. Для визначення рівня безпеки потрібно виконати оцінку ризиків функціонування кожної окремої складової, що буде розвиватися і вдосконалюватися в процесі розвитку системи.

За узагальнений показник рівня безпеки ІС можна взяти комплексну оцінку ризику. Для обчислення ризику використовують статистичну оцінку [7]:

$$R = \sum_{j}^{N} P_j g_j, \tag{1}$$

де P_j – ймовірність j-го варіанту подій, $(0 \le P_j \le 1)$, $\sum_j P_j = 1$;

g_j – втрати від реалізації *j*-го варіанту подій.

Визначення рівня безпеки грунтується на прогнозуванні процесу розвитку ІС та появи небезпек. Низка досліджень показала, що S-подібна логістична крива з високою ймовірністю описує розвиток різних систем [8, 9, 10, 11]. Кожен із параметрів системи, що розвивається, можна описати виразом:

$$S(t) = \frac{K \cdot S_0 e^{rt}}{K + S_0\left(e^{rt} - 1\right)}, \qquad (2)$$

де r – параметр, що характеризує швидкість росту (розвитку), K –максимальна границя параметра, S_0 – початкове значення, $S(t)$ – значення параметра на момент часу t.

Події, які можуть стати чинниками небезпеки інформаційних систем, перераховані в [12], але вони кардинально відрізняються від тих, що можуть стати причиною порушень безпеки ІС, що розвивається:

– зниження рівня надійності при збільшенні складності системи, якщо тільки це ускладнення не пов'язане з введенням елементів, спеціально призначених для підвищення надійності (резервних потужностей);

– впровадження нового програмного забезпечення, що розширює функції системи, може приводити до боротьби програм за ресурси системи, а ці ресурси завжди є обмеженими;

– зниження захищеності системи від вірусних, хакерських та інших атак при збільшенні кількості каналів доступу та чисельності персоналу.

Мета

Основною метою даної статті є удосконалення підходу до визначення рівня безпеки системи, що розвивається.

Розв’язання задач

Розрахунок ризику повинен базуватися на прогнозі розвитку структури ІС, її функцій, кількості інформації, що зберігається, кількості запитів, їх складності з одного боку та інтенсивності і небезпеки атак (хакерських, вірусніх та ін.) з іншого.

Зростання кількості доменів в зоні COM відображає історію розвитку Інтернету за останні роки [13]. Як видно з рис.1, бурхливе зростання кількості доменних імен в зоні COM в період з 1998-го по 2001 рік (період росту доткомів – період «зростання»), 2001-2002 більш стабільні значення (фаза «насичення»), сповільнився у 2002-му, в 2003 році відбувся спад (фаза «згасання»), а на початку 2004-го відновилося зростання реєстрацій (фаза «зародження» нового життєвого циклу).

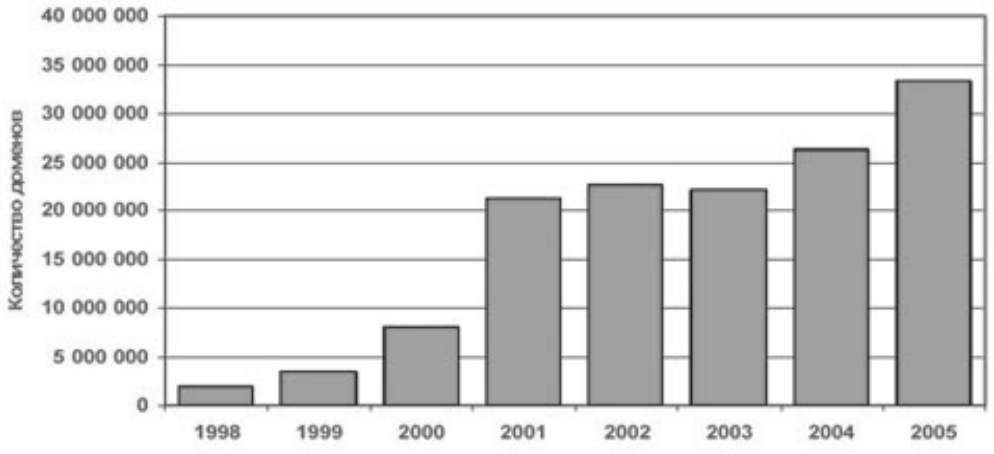

Рисунок 1 – Кількість зареєстрованих доменних імен другого рівня в домені COM в період з 1.01.1998 р. по 1.01.2005 р. (джерело: RU-CENTER). K –максимальна кількість доменних імен другого рівня, що може бути створена, r – параметр, що характеризує швидкість росту (розвитку), S_0 – початкова кількість доменних імен, S – кількість доменних імен на момент часу t.

Розвиток Інтернету у світі можна прослідкувати з графіка, представленого на рис.2.

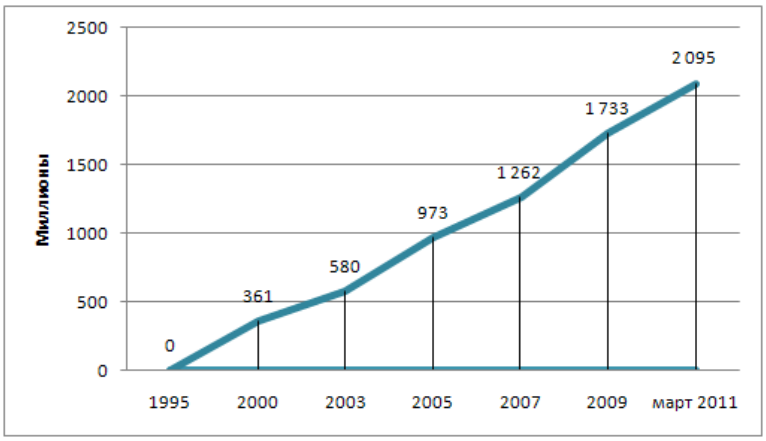

Рисунок 2 - Розвиток Інтернету у світі

З рис.1 і 2 видно, що процес розвитку може бути поданий послідовними фрагментами логістичної кривої. Таким чином, процес розвитку ІС можна подати системою рівнянь

$$\begin{cases} n(t) = \text{int}\left[\dfrac{t}{T}\right]; \\ \tau(t) = t - n(t)\cdot T; \\ S'(\tau) = \dfrac{K\cdot S_0 e^{r\tau}}{K + S_0\left(e^{r\tau} - 1\right)}; \\ S(t) = S'(T)\cdot n(t) + S'(\tau), \end{cases} \qquad (3)$$

де T - інтервал дії одної ділянки типу логістичної кривої; $\text{int}[\bullet]$ - функція виділення цілої частини аргументу; $n(t)$ - номер ділянки логістичного типу; $\tau(t)$ - інтервал часу від початку чергової ділянки логістичного типу; $S'(\tau)$ - окрема ділянка логістичного типу; $S(t)$ - крива розвитку.

Враховуючи особливість розвитку ІС, яка полягає у постійному пришвидшенні процесів розвитку, інтервал ділянки логістичної кривої будемо розглядати як функцію вигляду $T = T_0 \Big/ [n(t)]^{\nu}$, де ν – показник темпу прискорення. Параметри K, S_0, T, r підлягають ідентифікації для кожного процесу розвитку окремого параметру ІС.

Небезпеку несуть не тільки самі атаки, але й неузгодженість окремих аспектів розвитку, що призводить до порушення здатності ІС протистояти атакам і виконувати свої функції.

Для оцінювання ризику порушення безпеки за формулою (1) необхідно отримати оцінки ймовірностей *P* варіантів порушення безпеки в результаті неузгодженого розвитку окремих параметрів ІС. Очевидно, залежність ймовірності $P(\overline{x})$ від параметрів ІС повинна задовольняти умови:

- область визначення $0 \le \overline{x} < \infty$;
- область значень $0 \le P(\overline{x}) \le 1$;
- вектор параметрів $\overline{x}$ складається з двох підмножин: підмножини $\overline{x}_1$ параметрів, які менші за оптимальне значення $\overline{x}_{10}$, і підмножини $\overline{x}_2$ тих, які більші за оптимальне значення $\overline{x}_{20}$. Відповідно, збільшення значень $\overline{x}_1$ буде зменшувати ймовірність небезпеки, а збільшення $\overline{x}_2$ буде її збільшувати.

Апроксимуємо цю залежність функцією $P = e^{-k\frac{\overline{x}_1}{\overline{x}_2}}$, $\overline{x}_1 < \overline{x}_{10}$, $\overline{x}_2 > \overline{x}_{20}$, яка задовольняє усі умови і має додаткові переваги диференційованості на усій області визначення. Коефіцієнт k підлягає ідентифікації для кожної ІС і пари підмножин її параметрів $\{\overline{x}_1, \overline{x}_2\}$.

Вигляд апроксимуючої поверхні показаний на рис.3.

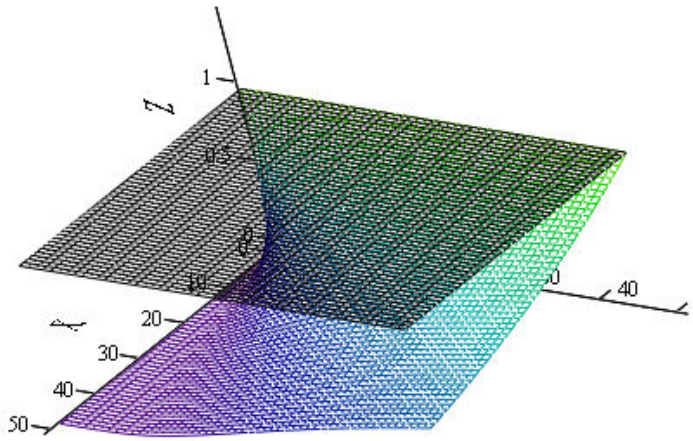

Рисунок 3 – Ймовірність втрати працездатності ІС при неузгодженому розвитку параметрів

Загальна ймовірність небезпеки

$$P_{dang} = 1 - \prod_i (1 - P_i), \tag{4}$$

де P_i – ймовірність небезпеки від кожного фактора.

Деякі фактори і характеристики небезпеки неузгодженого розвитку наведені у табл. 1 (наведений лише фрагмент таблиці).

Таблиця 1 – Фактори небезпеки неузгодженого розвитку

Параметри ІС, які розвиваються	**Параметри ІС, які розвиваються неузгоджено (уповільнено)**	**Характер небезпеки**	**Оцінка ймовірності небезпеки (апроксимована модель)**
1	2	3	4
Збільшення функцій	Розвиток системи захисту від атак	Ускладнення програмного забезпечення приводить до збільшення кількості точок вірусних і хакерських атак	$P = e^{-k_1 \frac{s_d}{n_f n_a}}$, де P - ймовірність втрати працездатності; n_f - кількість функцій; n_a - кількість атак; s_d - складність системи захисту; k_1 - коефіцієнт, який враховує розмірність величин та особливості конкретної ІС.
	швидкість обробки запитів	Затримка виконання процесів, перевантаження системи, відхилення запитів	$P = e^{-k_1 \frac{n_a}{n_f}}$, де P - ймовірність збоїв роботи; n_f - кількість функцій; n_a - швидкість обробки; k_1 - коефіцієнт, який враховує розмірність величин та особливості конкретної ІС.
	Обсяг пам’яті	Перевантаження системи, збої роботи	$P = e^{-k_1 \frac{s_d}{n_f n_a}}$, де P - ймовірність перевантаження системи; n_f - об’єм інформації, що вже зберігається; n_a - середній об’єм інформації, що зберігається при виконанні одної функції; s_d - об’єм пам'яті; k_1 - коефіцієнт, який враховує розмірність величин та особливості конкретної ІС.

продовження табл. 1

1	2	3	4
Збільшення кількості користувачів	Розвиток системи захисту від атак	Ускладнення програмного забезпечення приводить до збільшення кількості точок вірусних і хакерських атак	$P = e^{-k_1 \frac{n_a}{n_f}}$, де P - ймовірність втрати робочого часу; n_f - кількість користувачів; n_a - кількість атак; k_1 - коефіцієнт, який враховує особливості конкретної ІС.
	Необхідна швидкість обробки запитів	Затримка виконання процесів, перевантаження системи, відхилення запитів	$P = e^{-k_1 \frac{n_a}{n_f}}$, де P - ймовірність перевантаження системи; n_f - кількість користувачів; n_a - швидкість обробки запитів; k_1 - коефіцієнт, який враховує особливості конкретної ІС.
	Кількість каналів зв'язку	Перевантаження системи, збої роботи, Черги виконання операцій, втрата робочого часу	$P = e^{-k_1 \frac{n_a}{n_f}}$, де P - ймовірність перевантаження системи; n_f - кількість користувачів; n_a - швидкість обробки запитів; k_1 - коефіцієнт, який враховує особливості конкретної ІС.
	Необхідна швидкість каналів	Черги виконання операцій, втрата робочого часу	$P = e^{-k_1 \frac{n_a}{n_f}}$, де P - ймовірність втрати робочого часу; n_f - кількість користувачів; n_a - швидкість каналів; k_1 - коефіцієнт, який враховує особливості конкретної ІС.
	Необхідна швидкість обробки запитів	Затримка виконання процесів, перевантаження системи, відхилення запитів	$P = e^{-k_1 \frac{n_a}{n_f}}$, де P - ймовірність перевантаження системи; n_f - швидкість каналів; n_a - швидкість обробки запитів; k_1 - коефіцієнт, який враховує особливості конкретної ІС.
	Розвиток системи захисту від атак	Ускладнення програмного забезпечення приводить до збільшення кількості точок вірусних і хакерських атак	$P = e^{-k_1 \frac{n_a}{n_f}}$, де P - ймовірність втрати працездатності; n_f - швидкість каналів; n_a - кількість атак; k_1 - коефіцієнт, який враховує особливості конкретної ІС.
…	…	…	…

Оскільки, різноманітні фактори безпеки/небезпеки (див. вище) не являються незалежними, то проста адитивна формула (1) не підходить. Можна скористатися нечітким підходом на основі бази правил, оскільки метою роботи є отримання моделі для прогнозування ризиків розвитку ІС на основі комплексу факторів, кожен з яких змінюється у часі за законом (3), проте з різними параметрами.

Висновки

Розрахунок ризику базується на прогнозі розвитку структури ІС. Логістична крива використана при характеристиці розвитку різних сторін потенціалу ІС і її положення у зовнішньому середовищі. Будь-які зміни в ІС можуть приводити до погіршення рівня її безпеки. Небезпеку несуть не тільки атаки, але й неузгодженість окремих аспектів розвитку, що призводить до порушення здатності ІС виконувати свої функції. Наведені деякі фактори і характеристики небезпеки неузгодженого розвитку. Для розрахунку ймовірності небезпеки використана експоненційно-мультиплікативна апроксимація. Це дозволяє вра-

хувати як загрози безпеці, так і розвиток системи захисту, яка повинна включати як захист від атак, так і від структурно-параметрично-функціональних невідповідностей.

Список літератури

1. Information technology - Security techniques - Evaluation criteria for IT security -Part 1: Introduction and general model. -- ISO/IEC 15408-1.1999.
2. Information technology - Security techniques - Evaluation criteria for IT security -Part 2: Security functional requirements. -- ISO/IEC 15408-2.1999.
3. Information technology - Security techniques - Evaluation criteria for IT security -Part 3: Security assurance requirements. -- ISO/IEC 15408-3.1999.
4. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. -- М.: ИПК Издательство стандартов, 2002.
5. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.
6. Домарев В.В. "Безопасность информационных технологий. Методология создания систем защиты" – К.: ООО "ТИД "ДС", 2002 – 688 с.
7. Гранатуров В.М. Экономический риск. – М.: Дело и Сервис, 1999. – 112 с.
8. Дуброва Т.А. Статистические методы прогнозирования в экономике. /М. Московский международный институт эконометрики, информатики, финансов и права, 2003. – 50 с.
9. Мартино, Дж. Технологическое прогнозирование / Дж. Мартино. М. : Прогресс, 1977. – 591 с.
10. Красильников, О. Ю. Структурные сдвиги в экономике / О. Ю. Красильников. Саратов : Изд-во Саратов. гос. ун-та, 2001. – 171 с.
11. Альтшуллер, Г. С. Творчество как точная наука. ТРИЗ / Г. С. Альтшуллер.М. : Сов. радио, 1979. – 184 с.
12. Передерій Л.В. Системний аналіз безпеки інформаційних систем/Науковий вісник Донбасу. – 2010. – №1 (9). [електронний ресурс] Режим доступу до журналу: http://alma-mater.luguniv.edu.ua/magazines/elect_v/NN9/09plvbis.pdf
13. Internet World Stats. Usage and population statistic. [електронний ресурс] Режим доступу: www.internetworldstats.com

Відомості про авторів

Дубовой Володимир Михайлович – д.т.н., професор, завідувач кафедри КСУ, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021, тел. 59-81-57.
Дерман Галина Юріївна – аспірантка кафедри КСУ, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021, e-mail: fortyna1000@mail.ru.